

【特許請求の範囲】

【請求項 1】複数の暗号鍵の中から選択した暗号鍵を用いてデータを暗号化して暗号化データを生成し、当該選択した暗号鍵に対応する検索キーを当該暗号化データに付して送信する送信装置と、上記暗号化データを受信する受信手段と、上記複数の暗号鍵を記憶した鍵テーブルと、複数の検索キーと上記鍵テーブルにおける上記複数の暗号鍵との対応関係を記憶した検索テーブルと、上記検索キーを用いて上記検索テーブルを検索することにより、当該検索キーに対応する暗号鍵を上記鍵テーブルから取得する鍵検索手段と、上記取得した暗号鍵を用いて上記暗号化データを復号する復号手段とを有する受信装置とを具えることを特徴とする情報伝送システム。

【請求項 2】複数の暗号鍵の中から選択された暗号鍵を用いて暗号化された暗号化データを受信する受信手段と、上記複数の暗号鍵を記憶した鍵テーブルと、複数の検索キーと上記鍵テーブルにおける上記複数の暗号鍵との対応関係を記憶した検索テーブルと、上記暗号化データとともに送信される上記検索キーを用いて上記検索テーブルを検索することにより、当該検索キーに対応する暗号鍵を上記鍵テーブルから取得する暗号鍵検索手段と、上記取得した暗号鍵を用いて上記暗号化データを復号する復号手段とを具えることを特徴とする受信装置。

【請求項 3】上記暗号鍵検索手段は、上記暗号化データとともに送信される検索テーブル指定情報に基づいて複数の上記検索テーブルから 1 つの検索テーブルを選択し、上記検索キーを用いて当該選択した検索テーブルを検索することを特徴とする請求項 2 に記載の受信装置。

【請求項 4】上記暗号鍵検索手段は、上記暗号化データとともに送信される鍵テーブル指定情報に基づいて複数の上記鍵テーブルから 1 つの鍵テーブルを選択し、上記検索キーに対応する暗号鍵を当該選択した鍵テーブルから取得することを特徴とする請求項 2 に記載の受信装置。

【請求項 5】複数の暗号鍵を記憶した鍵テーブルと、複数の検索キーと上記鍵テーブルにおける上記複数の暗号鍵との対応関係を記憶した検索テーブルと、任意の上記検索キーを用いて上記検索テーブルを検索することにより、当該検索キーに対応する暗号鍵を上記鍵テーブルから取得する暗号鍵検索手段とを具えることを特徴とする暗号鍵検索装置。

【請求項 6】上記暗号鍵検索手段は、所定の検索テーブル指定情報に基づいて複数の上記検索テーブルから 1 つの検索テーブルを選択し、上記検索キーを用いて当該選択した検索テーブルを検索することを特徴とする請求項 5 に記載の暗号鍵検索装置。

【請求項 7】上記暗号鍵検索手段は、所定の鍵テーブル

指定情報に基づいて複数の上記鍵テーブルから 1 つの鍵テーブルを選択し、上記検索キーに対応する暗号鍵を当該選択した鍵テーブルから取得することを特徴とする請求項 5 に記載の暗号鍵検索装置。

【請求項 8】複数の検索キーと鍵テーブルが記憶する複数の暗号鍵との対応関係を記憶した検索テーブルを、任意の上記検索キーを用いて検索し、当該検索キーに対応する上記暗号鍵を上記鍵テーブルから取得することを特徴とする暗号鍵検索方法。

【請求項 9】所定の検索テーブル指定情報に基づいて複数の上記検索テーブルから 1 つの検索テーブルを選択し、上記検索キーを用いて当該選択した検索テーブルを検索することを特徴とする請求項 8 に記載の暗号鍵検索方法。

【請求項 10】所定の鍵テーブル指定情報に基づいて複数の上記鍵テーブルから 1 つの鍵テーブルを選択し、上記検索キーに対応する暗号鍵を当該選択した鍵テーブルから取得することを特徴とする請求項 8 に記載の暗号鍵検索方法。

【発明の詳細な説明】

【0000】

【発明の属する技術分野】本発明は情報伝送システム、受信装置、暗号鍵検索装置及び暗号鍵検索方法に関し、例えばデータを暗号化し衛星を介して伝送する情報伝送システムに適用して好適なものである。

【0000】

【従来の技術】従来ディジタル衛星放送システムにおいて、受信契約を行った正当な受信者のみが放送を受信し得る限定受信機構（CA: Conditional Access）が用いられている。

【0000】一般に限定受信機構においては、主に処理速度の問題から、送信側と受信側とで共通の暗号鍵を設定し、当該暗号鍵を用いて配信するデータストリームの暗号化及び復号化を行う共通鍵暗号化方式が適用されている。

【0000】かかる限定受信機構においては、受信契約を行った受信者に対して予め所定の暗号鍵を渡しておく。送信側はこの暗号鍵を用いて放送データを暗号化し、放送衛星を介して送信する。そして受信者は暗号鍵を用いて受信データの暗号化を解除することにより、受信契約を行った受信者のみが放送を視聴し得るようになっている。

【0000】暗号鍵は受信装置内部の記憶装置に記録されており、送信装置からの指示（例えば鍵の切り換えを指示する信号の送出や、暗号鍵の索引を特定し得るキーワードのデータストリームへの書き込み）に応じて、検索テーブル等の検索機構を用いて鍵を検索する。

【0000】ここで近年、ディジタル衛星放送システムを用いてデータ伝送を行う衛星データ伝送システムが実用化されている。衛星回線は電話回線や ISDN 回線等

に比べてその通信速度が速いため、大容量データを短時間で伝送することができという利点がある。

【0000】このような衛星データ伝送システムにおいて各受信者に対して個別のデータを伝送すると（これをユニキャスト通信と呼ぶ）、回線の利用効率が悪化してしまうという問題がある。このため衛星データ伝送システムにおいて、例えば受信者の属性等の適当な条件で複数の受信装置をグループ化し、同一のグループに属する受信装置に対して同報通信を行うことにより回線の利用効率を向上させる方法が考えられている。このようなグループに対する同報通信をマルチキャスト通信と呼ぶ。衛星データ伝送システムは本質的に同報性を有しているため、同報通信は容易に実現することができる。

【0000】個別通信と同報通信とでは受信装置におけるデータの処理方法が異なるため、鍵の索引となる識別符号の構成も異なる場合が多い。このため受信装置においては、どちらの通信方式でデータストリームが送信されているかを識別し、通信方式に応じた検索テーブルによって暗号鍵を検索する必要がある。

【0000】ここで、個別通信及び同報通信の両方に対応した受信装置においては、当該受信装置固有の個別鍵に加えて、所属するグループに割り当てられた共通鍵を持つ。そしてこの共通鍵はグループ毎に割り当てられているため、受信装置が複数のグループに所属している場合、所属するグループ全てについての共通鍵を持つ必要がある。

【0000】このため、このような個別通信及び同報通信の両方に対応した受信装置においては、個別鍵の検索テーブルと共通鍵の検索テーブルを持つことになり、構成が複雑になる、ひいては必要となる回路量も増大するという問題があった。

【0000】本発明は以上の点を考慮してなされたもので、簡易な構成で、様々な通信方法や暗号化方法に対応し得る情報伝送システム、受信装置、暗号鍵検索装置及び暗号鍵検索方法を提案しようとするものである。

【0000】

【課題を解決するための手段】かかる課題を解決するため本発明においては、複数の暗号鍵の中から選択した暗号鍵を用いてデータを暗号化して暗号化データを生成し、当該選択した暗号鍵に対応する検索キーと当該検索キーの属する検索テーブルを選択する信号とを当該暗号化データに付して送信する送信装置と、暗号化データを受信する受信手段と、複数の暗号鍵を記憶した鍵テーブルと、複数の検索キー及び前記暗号鍵との対応関係を記憶した検索テーブルと、検索キーを用いて検索テーブルを検索することにより当該検索キーに対応する暗号鍵を鍵テーブルから取得する鍵検索手段と、当該取得した暗号鍵を用いて暗号化データを復号する復号手段とを有する受信装置とを備えるようにした。

【0000】複数の暗号鍵を記憶した選択可能な鍵テ

ブルと、複数の検索キーと鍵テーブルにおける複数の暗号鍵との対応関係を記憶した検索テーブルとを設け、当該検索テーブルを検索キーで検索して鍵テーブルから暗号鍵を取得するようにしたことにより、簡易な構成で、様々な通信方法や暗号化方法に対応し得る情報伝送システムを実現できる。

【0000】

【発明の実施の形態】以下図面について本発明の一実施の形態を詳述する。

【0000】（１）衛星データ伝送システムの全体構成図１において、１は全体として本発明を適用した衛星データ伝送システムを示し、送信側システム２、衛星３、及び複数の同一構成でなる受信側システム４で構成される。送信側システム２と各受信側システム４とはそれぞれインターネット５を介して接続されている。また送信側システム２を管理するサービスプロバイダと各受信側システム４を所有する受信者との間では、予め当該衛星データ伝送システム１についての利用契約が結ばれている。

【0000】送信側システム２においては、当該送信側システム２全体を制御する制御装置１０、回線接続装置１１、データサーバ１２及び送信処理装置１３がローカルネットワーク１４を介して接続されている。

【0000】制御装置１０は、受信側システム４からインターネット５を介して送信されたデータ読出要求を回線接続装置１１を介して受信する。そして制御装置１０はデータ読出要求に応じて、データサーバ１２或いはインターネット５上のデータサーバ（図示せず）からデータを読み出し、送信処理装置１３に供給する。

【0000】送信処理装置１３は、供給されたデータをIP（Internet Protocol）パケット化した後暗号化し、さらに当該IPパケットを、DVB（digital Video Broadcasting）データ放送仕様（EN301 192）に準拠したセクションと呼ばれるデータブロックのペイロードに配置する。そして送信処理装置１３はセクションをMP EG（Moving Picture Experts Group）2方式に準拠した所定長のパケットに分割した後、各パケットにTSパケットヘッダを付することによりTS（Transport Stream）パケットを生成する。

【0000】ここで衛星データ伝送システム１においては、宛て先を識別する符号としてMPEG2-TS（Moving Picture Experts Group 2 Transport Stream）で規定するPID（Packet ID）や、受信側装置４の受信装置２１や情報処理装置２２の固有の識別番号として用いているMAC（Media Access Control：メディアアクセス制御）アドレスを利用している。そして送信処理装置１３は、衛星データ伝送システ

ム1で用いられる全ての暗号鍵を記述した鍵テーブルTkey、各グループのPIDと鍵テーブルTkeyに記憶された暗号鍵との対応関係を記述したPID検索テーブルT0、及び各受信装置21及び情報処理装置22それぞれのMACアドレスと鍵テーブルTkeyに記憶された暗号鍵との対応関係を記述したMACアドレス検索テーブルT1を有している。

【0000】制御装置10はPIDを用いて同報通信を行う場合はPID検索テーブルT0の使用を、MACアドレスを用いた個別通信の場合はMACアドレス検索テーブルT1の使用を送信処理装置13に指定する。送信処理装置13は指定された検索テーブルT0又はT1を用いてデータの送信先に応じた暗号鍵を検索し、当該検索した暗号鍵を用いて当該データを暗号化する。

【0000】このとき送信処理装置13は、各セクションに付せられたヘッダ（セクションヘッダ）内のCKI（Common Key Indicator、後述）の値を、例えば同報通信でPID検索テーブルT0を使用した場合は「0」、個別通信でMACアドレス検索テーブルT1を使用した場合は「1」とする。また送信処理装置13は、同報通信の場合、送信先グループに対応したPIDをTSパケットに付するのに対し、個別通信の場合、送信先装置のMACアドレスをセクションヘッダに記入する。

【0000】そして送信処理装置13は、かくして生成したTSパケットからトランスポートストリームを生成し、さらに変調、増幅等の処理を施して、送信アンテナ15を介してアップリンク波S2として衛星3に向けて送信する。

【0000】衛星3はアップリンク波S2を受信して増幅し、ダウンリンク波S3として地上の受信側システム4に向けて再送信する。

【0000】一方受信側システム4においては、受信装置21、回線接続装置23、及び、例えばパーソナルコンピュータ等なる複数の情報処理装置22が、ローカルネットワーク24を介して相互に接続されている。

【0000】受信装置21は、受信アンテナ20を介して受信したダウンリンク波S3に対して復調処理及び後述する復号処理を行うことにより、ローカルネットワーク24内の装置向けに送信されたデータを復号し、受信装置21に内蔵した記憶装置、ないしはローカルネットワーク24を介して情報処理装置22に供給する。

【0000】また情報処理装置22は、ユーザによってデータの読出要求操作が入力されると、これに応じてデータの読出要求を回線接続装置23及びインターネット5を介して送信側システム2に送信する。

【0000】（2）受信装置の構成
次に、受信側システム4の受信装置21を図2を用いて説明する。

【0000】受信装置21においては、当該受信装置2

1全体を制御するCPU（Central Processing Unit）30に、バス39を介してフロントエンド部31、デマルチプレクサ32、受信フィルタ33、復号部34、チェッカ35、バッファ36、鍵検索装置37及びインターフェース部38が接続されている。

【0000】フロントエンド部31は、受信アンテナ20を介して受信したダウンリンク波S3を復調し、トランスポートストリームD31としてデマルチプレクサ32に供給する。デマルチプレクサ32はトランスポートストリームD31からPIDに基づいて必要なTSパケットのみを分離し、受信フィルタ33に供給する。必要ならば受信フィルタ33は、TSパケットのヘッダ内容に基づいてデータ復号処理に不要なTSパケットを更に破棄し、残りのTSパケットを復号部34に供給する。

【0000】復号部34は後述する復号処理に基づいて動作し、これによって得られた検索情報をもって鍵検索装置37に問い合わせを行い、当該鍵検索装置37から暗号鍵を取得する。そして復号部34は、TSパケットを再構成してセクションを復元した後、鍵検索装置37から取得した暗号鍵を用いて当該セクションのペイロードを復号することにより、IPパケットとなる復号データストリームD34を得る。

【0000】必要ならば復号部34はチェッカ35に復号データストリームD34を供給し、正常に復号処理が行われたか否かを検定させる。これは例えば、送信側システム2から受信側システム4への暗号鍵の受け渡しが正常に行われなかったなどの理由により、誤った暗号鍵によって復号処理が行われた場合を想定しており、例えば送信処理装置13に入力するデータ列に対してCRC（Cyclic Redundancy Code）等の検査符号を付加した上で暗号化処理を行い、チェッカ35は復号データストリームD34において算出されたCRCの値が復号されたCRCの値と合致することによって処理が正常に完了したと判定する。なお、このチェッカ35の動作は付加機能であり、その存在の有無は本発明の効果には影響しない。そしてチェッカ35の処理を行わないのであれば、復号部34は復号データストリームD34をバッファ36に直接供給する。

【0000】上述したフロントエンド部31からチェッカ35に至るまでの処理はCPU30の処理とは独立して行われ、このためチェッカ35が復号データストリームD34を出力可能な瞬間に、CPU30が当該復号データストリームD34を処理可能であるとは限らない。このタイムラグを調整するため、バッファ36は復号データストリームD34を一時的に蓄積する。バッファ36に蓄積された復号データストリームD34は、CPU30の制御に応じて読み出されインターフェース部38に入力され、ローカルネットワーク24（図1）を介して情報処理装置22に供給される。

【0000】(3) 受信装置における復号処理

上述したようにセクションにおいては、ペイロードの先頭にセクションヘッダが付加されている。DVBデータ放送仕様(EN 301 192)によれば、セクションヘッダのビットの割り付けは図3に示す通りであり、各データバイトは走査線順に送信される。ここでMACアドレス#6とは、MACアドレスの最上位ビットをBit 47、最下位ビットをBit 0としたときの、Bit 7からBit 0を含むバイト(8bit)を意味する。

【0000】本発明による衛星データ伝送システム1においては、特開2001-136159で示された衛星データ伝送システムと同様に、セクションヘッダ6バイト目の最上位ビット(図3の2行めの第2番目のバイトのD7)をCKIと定める。そして衛星データ伝送システム1においては、上述したようにCKIの値を、同報通信でPID検索テーブルT0を使用した場合は

「0」、個別通信でMACアドレス検索テーブルT1を使用した場合は「1」とする。

【0000】ここで、DVBデータ放送仕様においては、CKIは「Reserved」とされており、値として「1」をとるように定められている。PIDを用いた同報通信はMACアドレスを用いた個別通信に比べてより特殊な処理方法であると考えられるので、同報通信のときにCKIを「0」とすると定めることで、DVBデータ放送仕様との仕様を一致することができる。さらに、特開2001-136159で示された衛星データ伝送システムにおいては、本願発明と同様に同報通信で共通鍵を使用した場合にCKIを「0」とし、個別通信で個別鍵を使用した場合にCKIを「1」とするようになされており、このため特開2001-136159で示された衛星データ伝送システムを容易に拡張して本願発明に適用することができる。

【0000】受信装置21の復号部34は、セクションヘッダのCKIの値に基づいて通信方式を判別する。そして復号部34は鍵検索部37に対して問い合わせを行い、CKIが「0」で同報通信の場合、TSパケットのPIDを検索キーとしてこれに対応する暗号鍵をPID検索テーブルT0から検索し、CKIが「1」で個別通信の場合、セクションヘッダのMACアドレスを検索キーとしてこれに対応する暗号鍵をMACアドレス検索テーブルT1を用いて検索する。

【0000】図4は鍵検索部37の構成を示し、上述したPID検索テーブルT0、MACアドレス検索テーブルT1及び鍵テーブルTkeyを有しているとともに、当該検索テーブルT0又はT1の一方を選択するセクタ37Aを有している。

【0000】鍵テーブルTkeyはp個のレコードを有しており、各レコードには暗号鍵が記録されている。ここで實際上衛星データ伝送システム1においては、Ev

en期間とOdd期間の2つの暗号鍵系列を有しており、これらをセクションヘッダの特定のビットに従って切り換えて使用することにより、暗号鍵の更新等を高速に実行し得るようになされている。このため鍵テーブルTkeyは、Even期間の暗号鍵(「KeyE」で示す)を格納した鍵テーブルTkeyEと、Odd期間の暗号鍵(「KeyO」で示す)を格納した鍵テーブルTkeyOとで構成される。このような仕組みについても本発明は問題なく適用できる。

【0000】また、PID検索テーブルT0においてはn個のレコードを有しており、それぞれに検索キーとしてのPIDの値と、鍵テーブルTkey内における当該PIDに対応した暗号鍵の位置(例えばレコード番号)を示す位置指定値Kpが記録されている。同様にMACアドレス検索テーブルT1においてはm個のレコードを有しており、それぞれに検索キーとしてのMACアドレスの値と、鍵テーブルTkey内における当該MACアドレスに対応した暗号鍵の位置を示す位置指定値Kpとが記録されている。なお、Kp[x][y]は、テーブルxの第y行目のレコードを示すものである。

【0000】ここで検索テーブルT0及びT1においては、異なる検索キーに対して同一値の位置指定値Kpが対応付けられていてもかまわない。例えば、複数のMACアドレスに対して同一の暗号鍵を割り当てる場合、これらのMACアドレスに対する位置指定値Kpは同一値となる。

【0000】なお、鍵テーブルTkey内の各暗号鍵、PID検索テーブルT0内の各PID及び各位置指定値Kp、並びにMACアドレス検索テーブルT1内の各MACアドレス及び各位置指定値Kpには、それぞれ有効/無効を表すValidビット(「V」で示す)が設けられており、それぞれの有効/無効を独立して設定し得るようになされている。なおValidビットは、その値が「1」の時有効とし、「0」の時無効とする。また、Even期間の鍵テーブルTkeyEを用いて暗号化した場合、後述するPSC(Payload Scrambling Control)の上位ビットの値を「0」とし、Odd期間の鍵テーブルTkeyOを用いて暗号化した場合、PSCの上位ビットの値を「1」とする。

【0000】このように鍵検索部37は、暗号鍵の実体を記憶した鍵テーブルTkeyと、当該鍵テーブルTkey内の各暗号鍵と検索キー(PID又はMACアドレス)との対応関係を記述したPID検索テーブルT0及びMACアドレス検索テーブルT1とを有している。このため鍵検索部37は、PID検索テーブル及びMACアドレス検索テーブルそれぞれに鍵フィールドを設ける場合に比べ、鍵検索部37の回路規模を削減することができる。

【0000】鍵検索部37のセクタ37Aは、CKI

が「0」のときPID検索テーブルT0を選択する。そして鍵検索部37はTSパケットのPIDを検索キーとしてPID検索テーブルT0を検索し、PIDの値が合致するレコードに記録された位置指定値Kpが示す暗号鍵を鍵テーブルTkeyから読み出して復号部34に供給する。また鍵検索部37のセレクタ37Aは、CKIが「1」のときMACアドレス検索テーブルT1を選択する。そして鍵検索部37はセクションヘッダのMACアドレスを検索キーとしてMACアドレス検索テーブルT1を検索し、MACアドレスの値が合致するレコードに記録された位置指定値Kpが示す暗号鍵を鍵テーブルTkeyから読み出して復号部34に供給する。

【0000】そして復号部34は、かくして得た暗号鍵を用い、セクションのペイロードに配置されたIPパケットを復号する。

【0000】(4) 復号処理手順

次に、受信装置21における復号処理手順を図5のフローチャートを用いて説明する。

【0000】復号部34はRT1で処理を開始し、ステップSP1において、セクションヘッダに記述されているMACアドレスをレジスタMRに代入するとともに、TSパケットのPIDをレジスタPRに代入し、次のステップSP2に進む。

【0000】ステップSP2において復号部34は、セクションヘッダにおけるPSC(Payload Scrambling Control)(図3)の下位ビットの値を参照し、当該セクションのペイロードのデータ(すなわちIPパケット)が暗号化されているか否かを判断する。ステップSP2において否定結果が得られた場合、このことは下位ビットが「0」であり、当該セクションのペイロードに配置されたIPパケットが暗号化されていないことを表しており、復号部34はステップSP12へ進み、暗号解除処理を行わずにセクションを後段のチェッカ35に送出し処理を終了する。

【0000】これに対してステップSP2において肯定結果が得られた場合、このことはPSCの下位ビットが「1」であり、当該セクションのペイロードに配置されたIPパケットが暗号化されていることを表しており、復号部34はステップSP3に進む。

【0000】ステップSP3において復号部34は、セクションヘッダにおけるCKI(図3)の値に基づいて、PID検索テーブルT0を用いて暗号鍵を検索すべきか、MACアドレス検索テーブルT1を用いて暗号鍵を検索すべきかを判断する。ステップSP3において肯定結果が得られた場合、このことはCKIが「0」であり、当該セクションが同報通信のセクションで、PID検索テーブルT0を用いて暗号鍵を検索すべきことを表しており、復号部34はステップSP4へ進む。

【0000】ステップSP4において、復号部34は鍵検索部37に対して問い合わせを行い、レジスタPRに

記憶されているPIDの値を検索キーとしてPID検索テーブルT0を検索する。鍵検索部37におけるPID検索テーブルT0の検索は、当該PID検索テーブルT0の先頭レコードから順に、PIDフィールド及び位置指定値フィールド双方が有効(すなわち双方のValidビットがともに「1」)なレコードに対してPIDが合致するまで行われる。

【0000】そして復号部34は、PID検索テーブルT0内にPIDが合致するレコードが存在しなかった場合、ステップSP11に移って当該セクションを破棄した後、ステップSP12に移って当該セクションに対する処理を終了する。

【0000】これに対して復号部34は、PID検索テーブルT0内にPIDが合致するレコードが存在した場合、ステップSP5に移って当該合致したレコードの位置指定値Kp[0][y]をレジスタKpに代入し、ステップSP8に移る。

【0000】一方、ステップSP3において否定結果が得られた場合、このことはCKIが「1」であり、当該セクションが個別通信のセクションで、MACアドレス検索テーブルT1を用いて暗号鍵を検索すべきことを表しており、復号部34はステップSP6へ進む。

【0000】ステップSP6において復号部34は鍵検索部37に問い合わせを行い、レジスタMRに記憶されているMACアドレスの値を検索キーとしてMACアドレス検索テーブルT1を検索する。鍵検索部37におけるMACアドレス検索テーブルT1の検索はステップSP4と同様に、当該MACアドレス検索テーブルT1の先頭レコードから順に、MACアドレスフィールド及び位置指定値フィールド双方が有効なレコードに対してMACアドレスが合致するまで行われる。

【0000】そして復号部34は、MACアドレス検索テーブルT1内にMACアドレスが合致するレコードが存在しなかった場合、ステップSP11に移って当該セクションを破棄した後、ステップSP12に移って当該セクションに対する処理を終了する。

【0000】これに対して復号部34は、MACアドレス検索テーブルT1内にMACアドレスが合致するレコードが存在した場合、ステップSP7に移って当該合致したレコードの位置指定値Kp[1][y]をレジスタKpに代入し、ステップSP8に移る。

【0000】ステップSP8において復号部34は、PSCの上位ビットをレジスタEOに代入する。そして復号部34は、レジスタEOの値が「0」のとき、Even期間の鍵テーブルTkeyEから、レジスタKpの値に対応するEven期間の鍵KeyE[Kp]についてのValidビットをレジスタValidに代入するのに対し、レジスタEOの値が「1」のとき、Odd期間の鍵テーブルTkeyOから、レジスタKpの値に対応するOdd期間の鍵KeyO[Kp]についてのValid

i dビットをレジスタValidに代入し、次のステップSP9に移る。

【0000】ステップSP9において復号部34は、レジスタValidの値に基づいて、暗号鍵の有効／無効を判断する。ステップSP9において否定結果が得られた場合、このことはPID又はMACアドレスに対応する暗号鍵が存在するにもかかわらず、当該暗号鍵が無効状態にあることを表しており、復号部34はステップSP11に移って当該セクションを破棄した後、ステップSP12に移って当該セクションに対する処理を終了する。

【0000】これに対してステップSP9において肯定結果が得られた場合、このことはPID又はMACアドレスに対応する暗号鍵が存在し、なおかつ当該暗号鍵が有効状態にあることを表しており、復号部34は次のステップSP10に移る。

【0000】ステップSP10において復号部34は、鍵テーブルTkeyからレジスタKp及びレジスタEOに対応する鍵データKey [Kp, EO]を取り出し、当該鍵データを用いてセクションのペイロードを復号し、ステップSP12に移って処理を終了する。

【0000】かくして復号部は、2つの異なる鍵検索方式に対応した復号処理を行う。

【0000】(5) 動作及び効果

以上の構成において、送信側システム2の送信処理装置13は、受信側システム4のデータ読み出し要求に応じたデータをデータサーバから読み出し、これをIPパケット化した後、さらに暗号化、セクション化及びTSパケット化し、アップリンク波S2として送信アンテナ15を介して衛星3に送信する。

【0000】このとき送信処理装置13は、送信するデータの通信形式が同報通信の場合、送信先グループに割り当てられたPIDに対応する暗号鍵をPID検索テーブルT0を用いて検索し、これにより得られた暗号鍵を用いて暗号化するとともに、当該PIDをTSパケットに記入し、さらにセクションヘッダ内のCKIの値を「0」とする。

【0000】これに対して送信処理装置13は個別通信の場合、送信先装置に割り当てられたMACアドレスに対応する暗号鍵をMACアドレス検索テーブルT1を用いて検索し、これにより得られた暗号鍵を用いて暗号化するとともに、当該MACアドレスをセクションヘッダに記入し、さらにCKIの値を「1」とする。

【0000】受信側システム4の受信装置21は、受信アンテナ39を介して受信したダウンリンク波S3を復調してトランスポートストリームD31を生成する。受信装置21の復号部34は、トランスポートストリームD31内のTSパケットからセクションを再構成する。

【0000】そして復号部34は、鍵検索部37に問い合わせを行い、セクションヘッダのCKIが「0」と

き、TSパケットのPIDを検索キーとしてPID検索テーブルT0を検索し、検索の結果得られた位置指定値Kpに対応する暗号鍵を鍵テーブルTkeyから取得し、当該暗号鍵を用いて当該受信装置21が属する同報グループ宛の同報通信を復号する。また復号部34は、セクションヘッダのCKIが「1」のとき、セクションヘッダに記入されたMACアドレスを検索キーとしてMACアドレス検索テーブルT1を検索し、検索の結果得られた位置指定値Kpに対応する暗号鍵を鍵テーブルTkeyから取得し、当該暗号鍵を用いて当該受信装置21宛の個別通信を復号する。

【0000】以上の構成によれば、暗号鍵の実体を記憶した鍵テーブルTkeyと、当該鍵テーブルTkey内の各暗号鍵と検索キーとの対応関係を記述した同報通信用のPID検索テーブルT0及び個別通信用のMACアドレス検索テーブルT1を鍵検索部37に設け、PID又はMACアドレスを検索キーとしてPID検索テーブルT0又はMACアドレス検索テーブルT1を検索し、当該検索キーに対応する位置指定値Kpに基づいて鍵テーブルTkeyから暗号鍵を取得するようにしたことにより、PID検索テーブル及びMACアドレス検索テーブルそれぞれに鍵フィールドを設ける場合に比べ、鍵検索部37の回路規模を削減することができる。

【0000】例えばDES (Data Encryption Standard) 方式の暗号化方式では、一般に48～128ビット長程度の暗号鍵が用いられる。これに対して、衛星データ伝送システム1において16個の暗号鍵を用いるとした場合、この全16個の暗号鍵を指定するための位置指定値Kpは4ビット長あれば良く、レコード内にフィールドとして直接鍵データを持つ場合に比べて検索テーブルのデータ量は格段に小さいものとなる。このため、2つの鍵テーブルを用いる場合に比べ、1つの鍵テーブルと2つの検索テーブルを用いた方が、回路規模を削減することができる。

【0000】また、検索テーブルを用いることにより、各鍵テーブル及び各検索テーブルのレコード数を独立かつ自由に決定することができ、これにより衛星データ伝送システム1のシステム設計に高い自由度を与えることができる。

【0000】例えば、検索テーブルを用いないとすると、複数のMACアドレスに対して同一の暗号鍵を割り当てる場合でも、鍵テーブルにはMACアドレスの個数と同じ数だけのフィールドを設ける必要がある。このフィールドには同一の暗号鍵を持つものが含まれる。これに対して検索テーブルを用いれば、鍵テーブルには暗号鍵の個数だけフィールドを設ければよい。

【0000】さらに、各検索テーブルのデータ構造は独立して決定し得るため、PIDとMACアドレスのような異なるビット長の検索キーを併用することが容易になり、また検索テーブルの修正も容易になる。

【0000】(6) 他の実施の形態

なお上述の実施の形態においては、衛星データ伝送システムに本発明を適用する場合について述べたが、本発明はこれに限らず、これ以外のデータ伝送システム、例えばケーブルインターネット等に適用しても良い。

【0000】また上述の実施の形態においては、同報通信と個別通信とを切り換えてデータ伝送する衛星データ伝送システムにおいて、2個の検索テーブルを使い分けて暗号鍵を検索するようにしたが、本発明はこれに限らず、通信方式の種類に応じて、3個以上の検索テーブルを使い分けて暗号鍵を検索するようにしたり、1個の検索テーブルを用いて暗号鍵を検索するようにしてもよい。

【0000】さらに上述の実施の形態においては、同報通信と個別通信とを切り換えてデータ伝送を行う衛星データ伝送システムにおいて、2個の検索テーブルと1個の鍵テーブルを設け、2個の検索テーブルのいずれか一方を用いて暗号鍵を検索するようにしたが、本発明はこれに限らず、単一の通信方法で2種類の暗号鍵系列を切り換えて暗号化を行う衛星データ伝送システムにおいて、1個の検索テーブルと2個の鍵テーブルを設け、当該2個の鍵テーブルのいずれか一方を用いて暗号鍵を検索するようにしてもよい。

【0000】図7はこの場合の鍵検索装置37の構成例を示し、1個の検索テーブルT0と、2個の鍵テーブルTkey0及び鍵テーブルTkey1とを有しているとともに、当該鍵テーブルTkey0及びTkey1の一方を選択するセレクタ37Bを有している。

【0000】検索テーブルT0は上述の実施の形態のPID検索テーブルT0(図4)と同様のデータ構成を有している。また鍵テーブルTkey0も、上述の実施の形態の鍵テーブルTkey(図4)と同様に、Even期間の鍵テーブルTkeyEとOdd期間のTkeyOとを有している。これに対して鍵テーブルTkey1はEven期間とOdd期間の区別がなく、さらに暗号鍵のビット長が鍵テーブルTkey0とは異なる。

【0000】送信側システム2の送信処理装置13(図1)は、制御装置10の制御に応じて鍵テーブルTkey0又はTkey1のどちらか一方を選択し、送信先の同報グループのPIDに対応した暗号鍵を用いてデータを暗号化した後送信する。

【0000】このとき送信処理装置13は、セクションヘッダ内に設けたKTS(Key Table Selection)の値を、鍵テーブルTkey0を使用した場合は「0」に、鍵テーブルTkey1を使用した場合は「1」とする。このKTSは、上述の実施の形態のCKIとは異なる場所に設けることが望ましい。例えば図6に示すように、セクションヘッダ6バイト目の2番目のビット(図6の2行目の第2番目のバイトのD6)をKTSと定めれば良い。

【0000】受信装置21の復号部34(図2)は鍵検索部37に対して問い合わせを行い、KTSが「0」の場合、PIDに対応する暗号鍵を鍵テーブルTkey0から検索し、KTSが「1」で個別通信の場合、PIDに対応する暗号鍵を鍵テーブルTkey1から検索する。

【0000】すなわち鍵検索部37のセレクタ37B(図7)は、KTSが「0」のとき鍵テーブルTkey0を選択する。そして鍵検索部37はTSパケットのPIDを検索キーとして検索テーブルT0を検索し、PIDの値が合致するレコードに記録された位置指定値Kpが示す暗号鍵を鍵テーブルTkey0から読み出して復号部34に供給する。また鍵検索部37のセレクタ37Bは、KTSが「1」のとき鍵テーブルTkey1を選択する。そして鍵検索部37はPIDを検索キーとして検索テーブルT0を検索し、PIDの値が合致するレコードに記録された位置指定値Kpが示す暗号鍵を鍵テーブルTkey1から読み出して復号部34に供給する。

【0000】そして復号部34は、かくして得た暗号鍵を用い、セクションのペイロードに配置されたIPパケットを復号する。

【0000】次に、この場合の復号処理手順を図8のフローチャートを用いて説明する。

【0000】復号部34はRT2で処理を開始し、ステップSP21においてTSパケットのPIDをレジスタPRに代入し、次のステップSP22に進む。

【0000】ステップSP22において復号部34は、セクションヘッダにおけるPSCの下位ビットの値を参照し、当該セクションのペイロードに配置されたIPパケットが暗号化されているか否かを判断する。ステップSP22において否定結果が得られた場合、このことは下位ビットが「0」であり、当該セクションのペイロードに配置されたIPパケットが暗号化されていないことを表しており、復号部34はステップSP31へ進み、暗号解除処理を行わずにセクションを後段のチェッカ35に送出し処理を終了する。

【0000】これに対してステップSP22において肯定結果が得られた場合、このことはPSCの下位ビットが「1」であり、当該セクションのペイロードに配置されたIPパケットが暗号化されていることを表しており、復号部34はステップSP23に進む。

【0000】ステップSP23において、復号部34は鍵検索部37に対して問い合わせを行い、レジスタPRに記憶されているPIDの値を検索キーとして検索テーブルT0を検索する。鍵検索部37における検索テーブルT0の検索は、当該検索テーブルT0の先頭レコードから順に、PIDフィールド及び位置指定値フィールド双方のValidビットがともに「1」なレコードに対してPIDが合致するまで行われる。

【0000】そして復号部34は、検索テーブルT0内

にPIDが合致するレコードが存在しなかった場合、ステップSP30に移って当該セクションを破棄した後、ステップSP31に移って当該セクションに対する処理を終了する。

【0000】これに対して復号部34は、検索テーブルTO内にPIDが合致するレコードが存在した場合、ステップSP24に移って当該合致したレコードの位置指定値Kp[0][y]をレジスタKpに代入し、ステップSP25に移る。

【0000】ステップSP25において復号部34は、セクションヘッダにおけるKTSの値に基づいて、鍵テーブルTkey0又はTkey1のどちらを用いて暗号鍵を検索すべきかを判断する。ステップSP25において肯定結果が得られた場合、このことはKTSが「1」であり、鍵テーブルTkey1を用いて暗号鍵を検索すべきことを表しており、復号部34はステップSP26へ進む。

【0000】ステップSP26において復号部34は、鍵テーブルTkey1から、レジスタKpの値に対応するKey[Kp]を取り出してレジスタKeyに代入するとともに、当該Key[Kp]についてのValidビットをレジスタValidに代入し、次のステップSP27に移る。

【0000】これに対してステップSP25において否定結果が得られた場合、このことはKTSが「0」であり、鍵テーブルTkey0を用いて暗号鍵を検索すべきことを表しており、復号部34はステップSP28へ進む。

【0000】ステップSP28において復号部34は、PSCの上位ビットをレジスタEOに代入する。そして復号部34はレジスタEOの値が「0」のとき、Even期間の鍵テーブルTkeyEからレジスタKpの値に対応するEven期間の鍵KeyE[Kp]を取り出してレジスタKeyに代入するとともに、当該KeyE[Kp]についてのValidビットをレジスタValidに代入するのに対し、レジスタEOの値が「1」のとき、Odd期間の鍵テーブルTkeyOからレジスタKpの値に対応するOdd期間の鍵KeyO[Kp]を取り出してレジスタKeyに代入するとともに、当該KeyO[Kp]についてのValidビットをレジスタValidに代入し、ステップSP27に移る。

【0000】ステップSP27において復号部34は、レジスタValidの値に基づいて暗号鍵の有効／無効を判断する。ステップSP27において否定結果が得られた場合、このことはPIDに対応する暗号鍵が存在するにもかかわらず、当該暗号鍵が無効状態にあることを表しており、復号部34はステップSP30に移って当該セクションを破棄した後、ステップSP31に移って当該セクションに対する処理を終了する。

【0000】これに対してステップSP27において肯

定結果が得られた場合、このことはPIDに対応する暗号鍵が存在し、なおかつ当該暗号鍵が有効状態にあることを表しており、復号部34は次のステップSP29に移る。

【0000】ステップSP29において復号部34は、レジスタKeyから鍵データを取り出し、当該鍵データを用いてセクションのペイロードを復号し、ステップSP31に移って処理を終了する。

【0000】かくして復号部34は、検索テーブルTOと、2つの鍵テーブルTkey0及び鍵テーブルTkey1とを用いて、2種類の異なる暗号鍵系列に対応した復号処理を行う。

【0000】以上の構成によれば、検索テーブルTOと、複数の鍵テーブルとを用いて暗号鍵を検索するようにしたことにより、複数の暗号鍵系列を使い分けて暗号化し得るとともに、それぞれの暗号鍵系列における暗号鍵のビット長を自在に設定でき、衛星データ送信システム1のシステム設計に高い自由度を与えることができる。

【0000】さらに本発明は、複数の通信方式及び複数の暗号鍵系列をそれぞれ選択して使用するようなデータ伝送システムに適用することもできる。この場合、通信方式の種類に応じた個数の検索テーブル及び暗号鍵系列の種類に応じた個数の鍵テーブルを用意するとともに、選択使用した検索テーブル及び鍵テーブルをそれぞれ指定し得るビット長の選択符号（例えば上述したCKI及びKTS）をセクションヘッダ内に設ければよい。この場合でも検索テーブル及び鍵テーブルの個数はそれぞれ独立して設定でき、システム設計に高い自由度を与えることができる。

【0000】

【発明の効果】上述のように本発明によれば、複数の暗号鍵を記憶した鍵テーブルと、複数の検索キーと鍵テーブルにおける複数の暗号鍵との対応関係を記憶した検索テーブルとを設け、当該検索テーブルを検索キーで検索して鍵テーブルから暗号鍵を取得するようにしたことにより、簡易な構成で、様々な通信方法や暗号化方法に対応し得る情報伝送システムを実現できる。

【図面の簡単な説明】

【図1】本発明による衛星データ伝送システムの全体構成を示すブロック図である。

【図2】受信装置の回路構成を示すブロック図である。

【図3】セクションヘッダの構成を示す略線図である。

【図4】鍵検索部の構成を示す略線図である。

【図5】復号処理を示すフローチャートである。

【図6】他の実施の形態のセクションヘッダの構成を示す略線図である。

【図7】他の実施の形態の鍵検索部の構成を示す略線図である。

【図8】他の実施の形態の復号処理を示すフローチャー

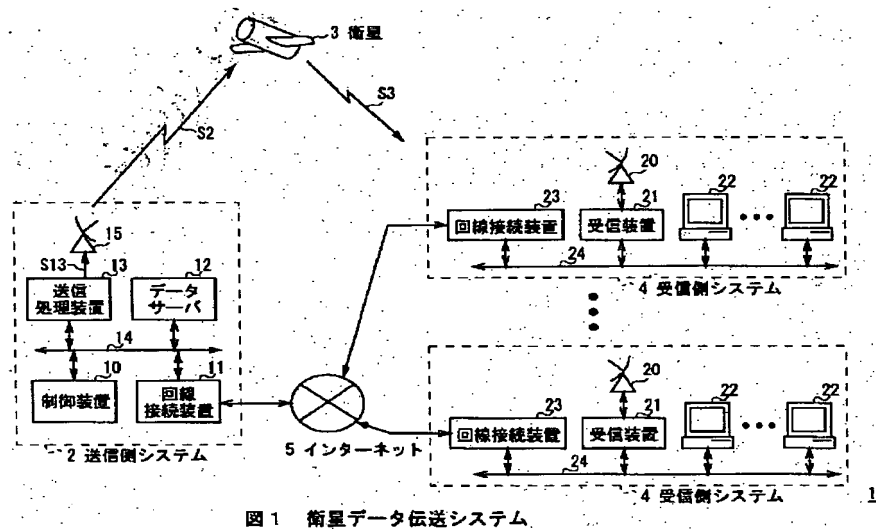
トである。

【符号の説明】

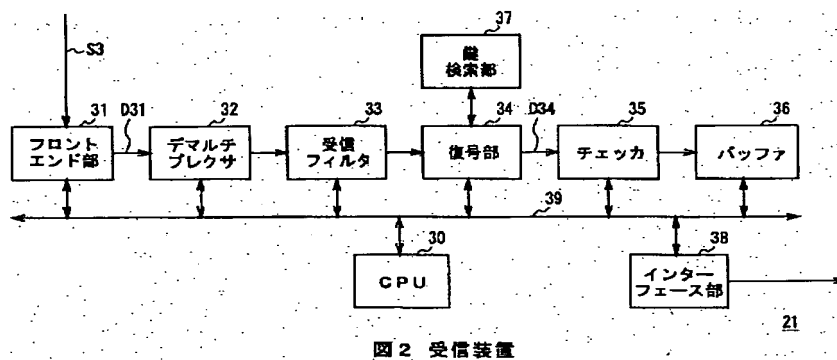
1……衛星データ伝送システム、2……送信側システム、3……衛星、4……受信側システム、5……インターネット、10……制御装置、11……回線接続装置、12……データサーバ、13……送信処理装置、14……ローカルネットワーク、15……送信アンテナ、20……受信アンテナ、21……受信装置、22……情報処理装置、23……回線接続装置、24……ローカルネットワーク、30……CPU、31……フロントエンド部、32……デマルチプレクサ、33……受信フィルタ、34……復号部、35……チェッカ、36……バッファ37……鍵検索装置、……インターフェース部、39……バス39。

……受信アンテナ20、21……受信装置、22……情報処理装置、23……回線接続装置、24……ローカルネットワーク、30……CPU、31……フロントエンド部、32……デマルチプレクサ、33……受信フィルタ、34……復号部、35……チェッカ、36……バッファ37……鍵検索装置、……インターフェース部、39……バス39。

【図1】



【図2】



【図3】

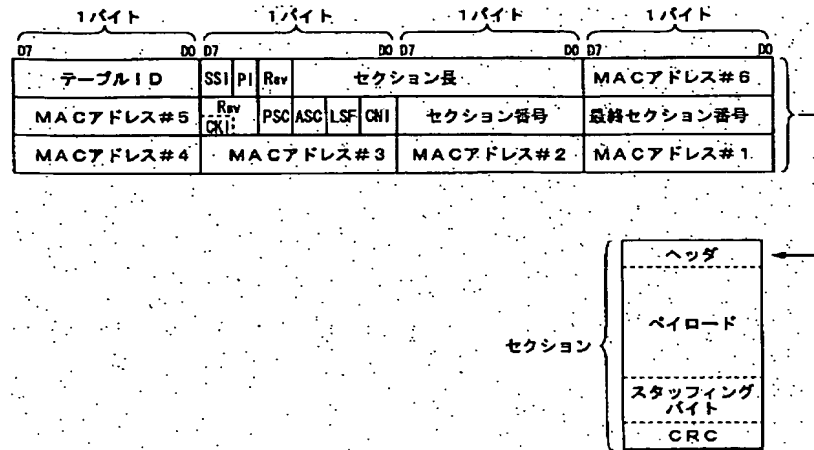


図3 セクションヘッダ

【図4】

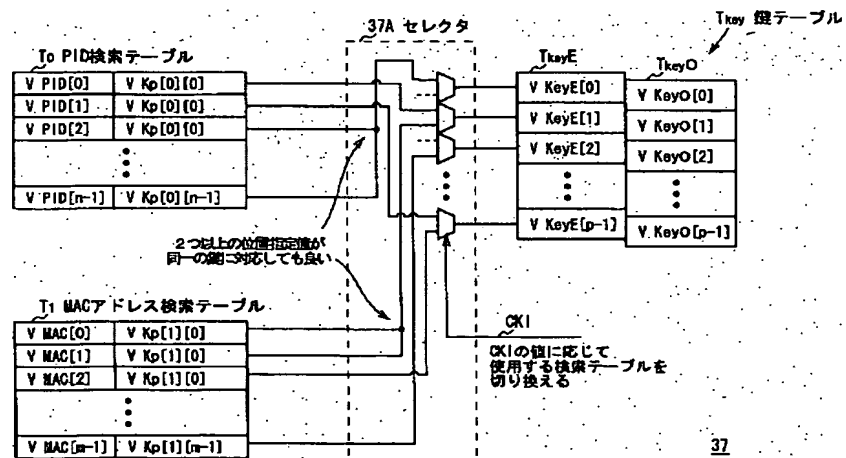


図4 鍵検索部の構成

【図5】

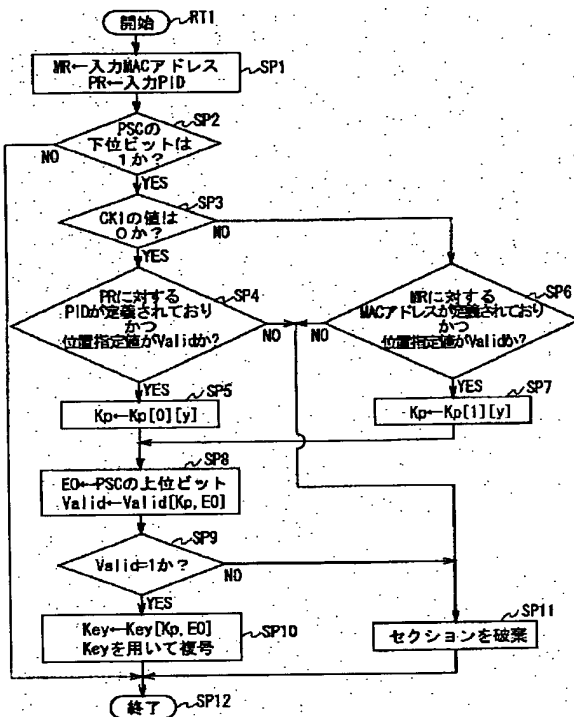


図5 復号処理手順

【図8】

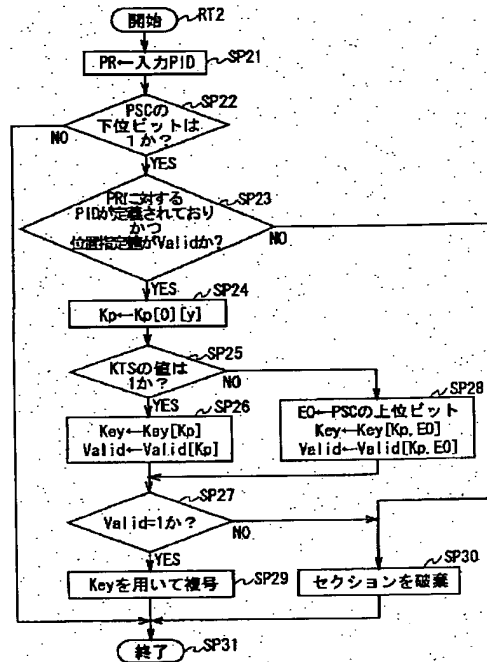


図8 他の実施の形態の復号処理

【図6】

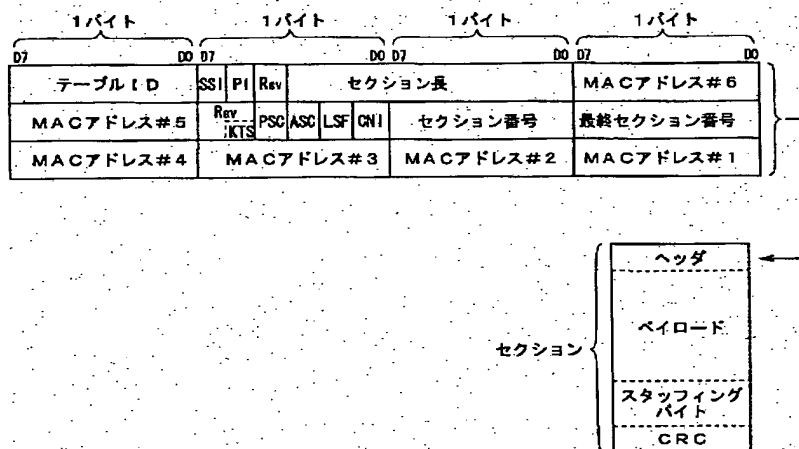


図6 他の実施の形態のセクションヘッダ

【図7】

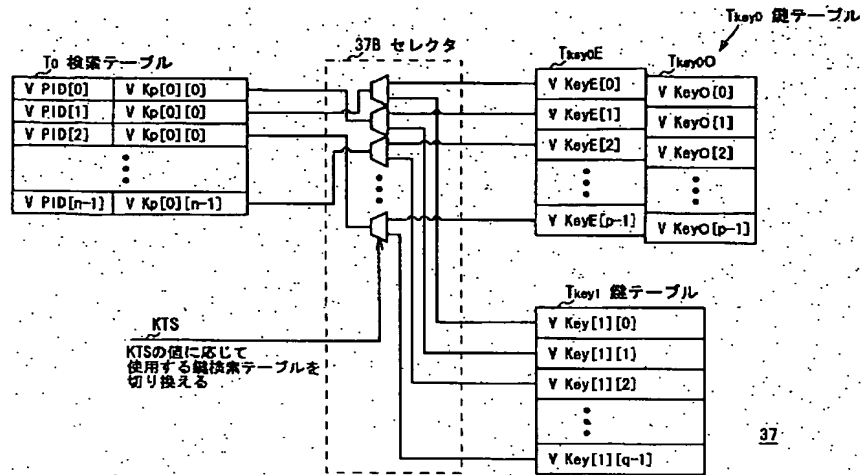


図7 他の実施の形態の鍵検索部の構成

THIS PAGE BLANK (USPTO)